

UNITED STATES DISTRICT COURT

for the
District of Maryland

FILED
LODGED
ENTERED
RECEIVED

OCT 23 2012

AT BALTIMORE
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND
DEPUTY

Case No. BY

12 2994 BPG

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

For information stored at premises owned, maintained,
controlled or operated by Yahoo!, Inc., associated with
accounts listed on Attachment A-3

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-3

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B-2

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Section 2251(a), (b)	Distribution of Child Pornography
18 U.S.C. Section 2252A(a)(2), (5)	Possession of Child Pornography

The application is based on these facts:

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Special Agent Jacqueline Dougher
Printed name and title

Sworn to before me and signed in my presence.

Date: 6-21-12

City and state: Baltimore, Maryland


Judge's signature

Beth P. Gesner, U.S. Magistrate Judge
Printed name and title

12 2994 BPG

ATTACHMENT A-3 - Yahoo!

This warrant applies to information associated with the following Yahoo! accounts:

1. odiejunior1954@yahoo.com;
2. othapalmerjr@yahoo.com;
3. malonfischer@yahoo.com;
4. edwoodfan41@yahoo.com;
5. lilbttman6969@yahoo.com;
6. eightanunder@yahoo.com;
7. lilbutsinc@yahoo.com; and
8. musicroom11@yahoo.com.

that are stored at premises owned, maintained, controlled, or operated by Yahoo!, a business with offices located at 701 First Avenue, Sunnyvale, California 94089.

12 2994 BPG

ATTACHMENT B-2 - AMERICA ONLINE AND YAHOO!

I. Search Procedure

1. The search warrant will be presented to the Internet Hosting Provider ("IHP") and its personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, the IHP employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. The IHP employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.

4. Law enforcement personnel will thereafter, using procedures described in Attachment C, review all information and records received from the IHP employees to determine the information to be seized by law enforcement personnel specified in Section III of Attachment B-2.

II. Files and Accounts to be Produced

A. All electronic mail stored and presently contained in, or on behalf of, the following electronic mail addresses listed in Attachments A-2 & A-3.

B. All existing printouts from original storage of all of the electronic mail described above in Section II A;

C. All transactional information of all activity of the electronic mail addresses described above in Section II (A), including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;

D. All business records and subscriber information, in any form kept, pertaining to the electronic mail address described above in Section II (A), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records; and

E. All records indicating the services available to subscribers of the electronic mail address described above in Section II (A).

12 2994 BPG

III. Information to be Seized by Law Enforcement Personnel

A. All electronic mail which is evidence, fruits, and instrumentalities of violations 18 U.S.C. § 2251(a) and (b) and 2252A(a)(2), specifically all electronic mail related to the following:

1. The production, distribution, or possession of child pornography.
 2. Videos, photographs, and other images contained on any of the accounts referenced in Attachment A-1 & A-2, including images of sexual conduct;
- B. All existing printouts from original storage which concern the categories identified in subsection III (A) and (B); and
- C. All of the records and information described above in Sections II (A) and (B);
- D. All "address books" or other lists of contacts.

10-12 2994 BPG

ATTACHMENT C

Description of Methods to be Used for Searching Computer-Related Items

This warrant authorizes the search of electronically stored information. The search shall be conducted pursuant to the following protocol in order to minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search are viewed.

With respect to the search of any digitally/electronically stored information seized pursuant to the instant warrant as described in Attachment A hereto, the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data to determine whether that data falls within the items to be seized;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized;
- c. surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized;
- d. opening or reading portions of files in order to determine whether their contents fall within the items to be seized;
- e. scanning storage areas to discover data falling within the list of items to be seized, to possibly recover any such deleted data, and to search for and recover files falling within the list of items to be seized; and/or
- f. performing key word searches through all electronic storage areas to determine whether occurrence of language contained in such storage areas exist that are likely to appear in the evidence to be seized.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the above listed crimes or other criminal activity, the further search of that particular directory, file or storage area, shall cease.